Data Security in the Latest “Year of the Healthcare Breach”

Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”), and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Introduction

Worldwide, healthcare represents a US$8 trillion industry—and unfortunately, that industry, like many others, suffers from unhealthy levels of cybersecurity threats and breaches. Reputable estimates hold that six percent of global healthcare spending—some US$480 billion at current levels—is lost each year to fraud, much of which involves compromised medical records.

In September 2015, Healthcare Informatics reported that in the first half of that year alone, the healthcare industry suffered 187 breaches, 21 percent of the 888 breaches reported worldwide. Those healthcare breaches resulted in 84.4 million compromised records, or 34 percent of the worldwide total of 246 million, according to that report.

As with most serious illnesses, the passage of time has not lessened the severity of the problem. In May 2016, eSecurity Planet reported that the Ponemon Institute's Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data found 89 percent of healthcare organizations were breached in the past two years. That same study found 45 percent of those organizations had been breached five or more times in the same two-year period.

Healthcare as a Target

Clearly, the worldwide healthcare industry is increasingly targeted by the worldwide hacking industry. There are two clear reasons for this: financial gain and opportunity.

Reason #1: financial gain. The black-market value of a credit card number has reportedly fallen to about $1 per record, as financial organizations have become better at securing their databases, thwarting threats, and remediating successful breaches. Meanwhile, the value of personally identifiable information (PII) such as Social Security or National Insurance numbers, is now worth 10 to 20 times that much, according to published reports. However, some hackers apparently offer “volume discounts.” A June 2016 eSecurity Planet report said a hacker was offering to sell 700,000 stolen records, including Social Security numbers and other PII, for $655,000. This may have been a “loss leader,” however. Other reports indicate this same hacker stole a total of 9.3 million such records.

When personal health information (PHI) is added to the equation, the value is even higher. Hackers or their sponsors can pose as doctors and use that PHI to file very profitable fraudulent insurance claims or order and resell controlled substances and medical equipment. Even without specific medical information, criminals can use PII to apply for loans. When combined with other information and counterfeit documents, PHI records can sell for as high as $500 each, according to a December 2014 Forrester Research report.

Reason #2: opportunity. When one type of target becomes hardened, hackers tend to refocus their efforts on less secure types. For example, after financial and retail organizations became better at securing centralized databases, hackers found ways to breach less-secure, retail point-of-sale (POS) systems. Healthcare systems are ripe for this “soft-target” approach, and have been for some time now. According to a warning issued in April 2014 by the US FBI and obtained by Reuters, “The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors. Therefore, the possibility of increased cyber intrusions is likely.” Current reality proves the prescience of that warning and provides two dominant reasons for its accuracy.

- From a cybersecurity perspective, healthcare IT environments are chaotic. PCs are shared by multiple doctors and nurses. Aging medical equipment relies on software that rarely or never gets updated, and exists on outdated, unpatched, and sometimes even unsupported operating systems. In many cases, the software provider may no longer exist, making security updates difficult or impossible.
- Healthcare providers, consumers, and administrators increasingly want and need to communicate, view, and share medical and other information when away from their primary work locations. Their remote laptops must be as well protected as the computers they use when at "the office." However, solutions for managing and securing those laptops and the information they access can be unwieldy and generate user resistance. That resistance often surfaces as users finding ways to "work around" tools and measures intended to keep them, their laptops, and critical corporate and private patient information secure. Some healthcare organizations struggle to limit or forbid remote access to their networks and information. Others allow such access but with little to no confidence in the security of those remote connections.

Essential Security Strategies

To enhance security significantly, healthcare organizations can and should harness two strategies. One is comprehensive operating system and software application patching. The other is securing access to PHI, PII, and other business-critical information for fixed-location and mobile users, their computers, and their applications. Both are relatively simple to implement and unlikely to generate user resistance.

Patch Management

Most breaches start with malware infection, and most malware infections exploit vulnerabilities in unpatched software. Comprehensive patching of operating systems and software applications is therefore essential for maximum security and for compliance with relevant laws, regulations, and business requirements. This is especially important in environments that include old and shared systems running many different types and versions of operating systems and software.

Many organizations have spent years perfecting their server operating system and Microsoft software patching strategy using essential tools such as Microsoft System Center Configuration Manager (SCCM). However, hackers seeking softer targets now focus their efforts on vulnerabilities in common, less-widely protected, third-party applications and browser add-ins, such as Adobe Acrobat Reader and Flash Player, Google Chrome, Mozilla Firefox, and Oracle Java. According to the Center for Strategic and International Studies, 75 percent of attacks use publicly known vulnerabilities in commercial software. The Verizon 2016 Data Breach Investigations Report (DBIR) states that the top 10 vulnerabilities account for 85 percent of all successful breaches. In 2015, the DBIR team found that many vulnerabilities date back to 2007. Attacks aimed at these and other vulnerabilities can be easily and consistently thwarted by regular patching.

Tools such as Microsoft SCCM excel at automated operating system patching. However, their abilities to patch third-party applications are insufficient.

Secure Information Access

Healthcare organizations looking to support mobile device use among doctors and other healthcare staff should start with a strategy that focuses on comprehensive, consistent protection of information. To be of maximum effectiveness and value, such a strategy must provide protection from ransomware and other threats hidden in email attachments, links, and other file types. That strategy must also provide effective protection against threats from rogue applications. Effective, granular controls over application access and privilege management offer user- and information-protection features that complement and enhance comprehensive patch management.

How Ivanti Can Help

Ivanti offers several essential tools for implementing a comprehensive software patching and information protection strategy:

1. **Ivanti Patch for SCCM** integrates tightly with Microsoft SCCM to extend its patch vulnerability detection and deployment to third-party applications. Using SCCM’s own patch delivery mechanism, Patch for SCCM monitors and patches hundreds of popular, third-party applications, including those of Adobe, Apple, Google, Java, and Firefox. The intuitive Patch for SCCM console plug-in eliminates the manual steps required to define and load patch information into SCCM.
2. **Ivanti Application Control for SCCM** enables IT admins to better comply with application policy and license agreements in SCCM environments, apply the most appropriate administrative rights level for each user, and block malware and ransomware at the endpoint. With Application Control for SCCM, IT admins can maintain end user control, increase user acceptance, and reduce helpdesk calls, without reliance on complex, high-maintenance scripts, blacklists, or whitelists.
3. **Ivanti Xtraction** is a self-service reporting and dashboard solution. It aggregates data from Microsoft SCCM and other sources with no coding required, and provides a drag-and-drop interface for easy report and dashboard creation. It complements and expands upon the reporting features of SCCM, to provide consolidated, actionable information about your security posture.

Conclusion

Where hackers are concerned, the worldwide healthcare industry is a prime target, but healthcare organizations can take steps today to ensure they are protected. A security strategy that encompasses automated, comprehensive application and operating system security patching, and secure information and application access can be cost-effective and implemented quickly. Such a strategy can provide comprehensive protection from both known and emerging threats and attacks.

www.ivanti.com

1.800.982.2130

sales@ivanti.com